The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
12/13/2011

SUBJECT:
Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS11-087)

OVERVIEW:
A vulnerability has been discovered in Microsoft Windows Kernel-Mode Driver. Exploitation of this vulnerability could result in the execution of arbitrary code with administrative privileges resulting in full control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

SYSTEMS AFFECTED:
- Microsoft Windows XP
- Microsoft Vista
- Microsoft Windows 7
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been identified in Microsoft Windows Kernel-Mode driver (win32.sys) that could allow for remote code execution. The "win32.sys" kernel-mode device driver provides various functions such as the window manager, collection of user input, and screen output. A remote code execution vulnerability exists in implementations of Microsoft Windows in which the kernel mode driver does not perform proper validation when writing TrueType fonts into a buffer.

This vulnerability has been used to drop the Duqu malware by embedding a malformed font inside an Office Word document. An attacker could take advantage of this issue by getting a user to open a specially crafted file containing malformed TrueType fonts via a website, email, or by hosting the file on a network share. Successfully exploitation will result in an attacker gaining the ability to install programs; view, change, or delete data; or create new accounts with full system rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the principle of Least Privilege to all services.

REFERENCES:

Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms11-087
http://blogs.technet.com/b/srd/archive/2011/12/13/more-information-on-ms11-087.aspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402

SecurityFocus:
http://www.securityfocus.com/bid/50462